DOCUMENT RESUME

ED 175 689 SE 028 677

AUTHOR Schaaf, William L., Ed.
TITLE Reprint Series: Prime Numbers and Perfect Numbers. RS-2.
INSTITUTION Stanford Univ., Calif. School Mathematics Study Group.
SPONS AGENCY National Science Foundation, Washington, D.C.
PUB DATE 66
NOTE 44p.; For related documents, see SE 028 676-690

EDRS PRICE MF01/PC02 Plus Postage.
DESCRIPTORS *Algebra: Curriculum: *Enrichment: *Instruction: Mathematics Education; *Number Concepts: *Prime Numbers; Secondary Education: *Secondary School Mathematics; Supplementary Reading Materials
IDENTIFIERS *School Mathematics Study Group

ABSTRACT

This is one in a series of SMSG supplementary and enrichment pamphlets for high school students. This series makes available expository articles which appeared in a variety of mathematical periodicals. Topics covered include: (1) the prime numbers: (2) mathematical sieves: (3) the factorgram: and (4) perfect numbers. (MP)

Printed in the United States of America

Financial support for the School Mathematics Study Group has been provided by the National Science Foundation.

Mathematics is such a vast and rapidly expanding field of study that there are inevitably many important and fascinating aspects of the subject which do not find a place in the curriculum simply because of lack of time, even though they are well within the grasp of secondary school students.

Some classes and many individual students, however, may find time to pursue mathematical topics of special interest to them. The School Mathematics Study Group is preparing pamphlets designed to make material for such study readily accessible. Some of the pamphlets deal with material found in the regular curriculum but in a more extended manner or from a novel point of view. Others deal with topics not usually found at all in the standard curriculum.

This particular series of pamphlets, the Reprint Series, makes available expository articles which appeared in a variety of mathematical periodicals. Even if the periodicals were available to all schools, there is convenience in having articles on one topic collected and reprinted as is done here.

This series was prepared for the Panel on Supplementary Publications by Professor William L. Schaaf. His judgment, background, bibliographic skills, and editorial efficiency were major factors in the design and successful completion of the pamphlets.

Panel on Supplementary Publications

R. D. Anderson (1962-66)	Louisiana State University, Baton Rouge
M. Philbrick Bridgess (1962-64)	Roxbury Latin School, Westwood, Mass.
Jean M. Calloway (1962-64)	Kalamazoo College, Kalamazoo, Michigan
Ronald J. Clark (1962-66)	St. Paul's School, Concord, N. H.
Roy Dubisch (1962-64)	University of Washington, Seattle
W. Eugene Ferguson (1964-67)	Newton High School, Newtonville, Mass.
Thomas J. Hill (1962-65)	Montclair State College, Upper Montclair, N. J.
L. Edwin Hirschi (1965-68)	University of Utah, Salt Lake City
Karl S. Kalman (1962-65)	School District of Philadelphia
Isabelle P. Rucker (1965-68)	State Board of Education, Richmond, Va.
Augusta Schurrer (1962-65)	State College of Iowa, Cedar Falls
Merrill E. Shanks (1965-68)	Purdue University, Lafayette, Indiana
Henry W. Syer (1962-66)	Kent School, Kent, Conn.
Frank L. Wolf (1964-67)	Carleton College, Northfield, Minn.
John E. Yarnelle (1964-67)	Hanover College, Hanover, Indiana

PREFACE

Throughout all history, men have been curious about the ordinary integers, or, more precisely, the natural numbers 1, 2, 3, 4, $\cdots$. Even little children are fascinated by numbers, as evidenced by their games and their verses: "One, two, buckle my shoe, etc."

The story of number theory begins with the ancient Greeks, for whom *arithmetiké* was the science of numbers rather than the art of computation. (Reckoning was called *logistica* and was generally deemed beneath the dignity of mathematicians and philosophers.) Thus Euclid, the Pythagoreans, and other Greek writers were familiar with prime numbers, perfect numbers, amicable numbers, and figurate numbers.

The classical theory dealt only with the natural numbers. The modern theory of numbers, however, studies the properties of the system of rational integers $0, \pm 1, \pm 2, \cdots$. An integer b is said to divide an integer a if there exists an integer k such that $a = bk$. We can say that a is divisible by b, or that b is a *factor* of a, also that a is a *multiple* of b and that k is the *quotient* of a by b, provided that $b \neq 0$.

A *unit* is an integer that divides every integer; e.g., $+1$ and -1. A prime number, or a *prime*, is an integer, not a unit, that is divisible only by itself and the units. For example, 2, 3, 5, 19, and 37 are primes. A composite number, or a *composite*, is an integer that is not zero, not a unit, and not a prime; for example, 4, 21, 91, and 111 are composites. All integers take the form 2n or 2n + 1. An *even* integer is one that is a multiple of 2; any integer that is not even is *odd*.

The theory of numbers differs somewhat from other fields of mathematics in several respects. In the first place, the beginner in number theory needs but little other preparatory mathematical knowledge as a background—the basic principles of algebra virtually suffice. In the second place, despite appearing to be relatively independent of other fields of mathematics and despite the innocent simplicity of the statement of many theorems, number theory is noted for the difficulty of its problems and proofs, which require considerable mathematical insight and ingenuity. To illustrate the apparent simplicity of some problems, consider the following theorems:

(1) Every positive integer is a sum of four squares, and fewer than four squares will not suffice.

For example: $7 = 2^2 + 1^2 + 1^2 + 1^2$

$22 = 4^2 + 2^2 + 1^2 + 1^2$

(2) Every integer n can be expressed in the form $n = x^2 + y^2 - z^2$

For example $7 = 2^2 + 2^2 - 1^2$

$22 = 5^2 + 1^2 - 2^2$

Such relations and properties are very simple to state and easy to understand, and are even readily illustrated by specific examples, but to give a general proof is often exceedingly difficult.

On the other hand, some properties are rather easy to prove. For example:

(1) The product of any two consecutive integers is divisible by 2.

(2) The sum of any integer and its square is an even number.

(3) The product of any three consecutive integers is divisible by 3.

Try to discover a proof for each of these by yourself!

This collection of essays explores, in a very elementary way, only two aspects of number theory, namely the primes and the perfect numbers.

—William L. Schaaf

CONTENTS

THE PRIME NUMBERS . . . . Howard W. Eves 3

MATHEMATICAL SIEVES . . . . David Hawkins 9

THE FACTORGRAM . . . . Kenneth P. Swallow 27

PERFECT NUMBERS . . . . Constance Reid 35

ACKNOWLEDGMENTS

The *SCHOOL MATHEMATICS STUDY GROUP* takes this opportunity to express its gratitude to the authors of these articles for their generosity in allowing their material to be reproduced in this manner: Professor Howard W. Eves, of the University of Maine; Mr. David Hawkins; Kenneth P. Swallow, who, when his article first appeared, was associated with the Newark (N. J.) College of Engineering; and Constance Reid, author and a frequent contributor to scholarly journals.

The *SCHOOL MATHEMATICS STUDY GROUP* is also pleased to express its sincere appreciation to the several editors and publishers who have been kind enough to allow these articles to be reprinted, namely:

THE MATHEMATICS TEACHER

Howard Eves, "The Prime Numbers," vol. 51 (March 1958), pp. 201–203.

Kenneth Swallow, "The Factorgram," vol. 48 (Jan. 1955), pp. 13–17.

THE SCIENTIFIC AMERICAN

David Hawkins, "Mathematical Sieves," vol. 199 (Dec. 1958), pp. 105–112.

Constance Reid, "Perfect Numbers," vol. 188 (March 1953), pp. 84–86.

FOREWORD

The theory of prime numbers can be a fascinating subject. One of the notable achievements of Greek mathematics is Euclid's proof that the number of primes is infinite. His proof is simple and, in the language of the mathematician, "elegant."

Another significant cornerstone of number theory is the *Fundamental Theorem of Arithmetic*, which states that, disregarding the order of the factors, a composite number can be factored into primes in one and only one way. For example:

(1) $66 = 2 \cdot 3 \cdot 11$

(2) $96 = 2^5 \cdot 3$

(3) $1323 = 3^3 \cdot 7^2$

It should be noted that in the field of number theory there are many unsolved problems as well as some "theorems" which are believed to be true, but for which no proof has as yet been given. Thus, although it has been proved that the number of primes is infinite, the problem of finding the *next* prime after any given prime still remains unsolved. Nor has anyone succeeded in developing a general method for finding even one prime number greater than a given one. Again, it is suspected that every positive even integer can be represented as the difference of two positive primes in infinitely many ways, but this has never been proved. For example:

(1) $6 = 11 - 5 = 13 - 7 = 17 - 11 = 19 - 13 =$ etc.

(2) $8 = 11 - 3 = 13 - 5 = 19 - 11 = 31 - 23 =$ etc.

Perhaps one of the most celebrated unsolved problems of number theory is the well-known Goldbach's conjecture—every even integer greater than 2 can be represented as the sum of two positive primes. For example:

(1) $4 = 2 + 2$

(2) $10 = 3 + 7 = 5 + 5$

(3) $30 = 11 + 19 = 7 + 23$

(4) $100 = 11 + 89 = 17 + 83 = 41 + 59$

Here is indeed a fascinating and challenging topic!

by Ernst Meissel, who succeeded in showing that the number of primes below 10^8 is 5,761,455. The Danish mathematician Bertelsen continued these computations and announced, in 1893, that the number of primes below 10^9 is 50,847,478. This represents our most extended knowledge along these lines.

No practicable procedure is yet known for testing large numbers for primality, and the effort spent on testing certain special numbers has been enormous. For more than 75 years the largest number actually verified as a prime was the 39-digit number

$$2^{127} - 1 = 170,141,183,460,469,231,731,687,303,715,884,105,727,$$

given by the French mathematician Anatole Lucas in 1876. In 1952, the EDSAC machine, in Cambridge, England, established the primality of the much larger (79-digit) number

$$180\,(2^{127} - 1)^2 + 1,$$

and in the same year the SWAC digital computer, in the United States, established the primality of the enormous numbers $2^{521} - 1$, $2^{607} - 1$, and $2^{1279} - 1$, the last of which is a 386-digit number.

A dream of number theorists is the finding of a function $f(n)$ which will yield prime numbers for all positive integral n. Thus $f(n) = n^2 - n + 41$ yields primes for all such $n < 41$, but $f(41) = (41)^2$, a composite number. The quadratic polynomial $f(n) = n^2 - 79n + 1601$ yields primes for all $n < 80$. Polynomial functions can be obtained which will successively yield as many primes as desired, but no such function can be found which will always yield primes. It was about 1640 that the great number theorist, Pierre de Fermat, conjectured that $f(n) = 2^{2^n} + 1$ is prime for all nonnegative integral n. For $n = 0, 1, 2, 3, 4$ we find $f(n) = 3, 5, 17, 257, 65537$, all prime numbers, but in 1732 Euler proved the conjecture false by showing that $f(5) = (641)(6700417)$. It is now generally felt that $f(n)$ is composite for all other values of n, although this has not been established. An interesting recent result along these lines is the proof, by W. H. Mills in 1947, of the existence of a real number A such that the largest integer not exceeding A^{3^n} is a prime for every positive integer n. Nothing was shown about the actual value, nor even the rough magnitude, of the real number A.

A remarkable generalization of Euclid's theorem on the infinitude of the primes was established by Lejeune-Dirichlet (1805–59), who succeeded in showing that every arithmetic sequence,

$$a, a + d, a + 2d, a + 3d, \cdots,$$

in which a and d are relatively prime, contains an infinitude of primes. The proof of this result is far from elementary.

Perhaps the most amazing result yet found concerning the distribu-

The Prime Numbers*

Howard W. Eves

Proposition 14 of Book IX of Euclid's *Elements* is essentially the equivalent of the important "fundamental theorem of arithmetic," which states that *any integer greater than 1 can, except for the order of the factors, be expressed as a product of primes in one and only one way.* This theorem asserts that the prime numbers are building bricks from which all other integers may be made. Accordingly, the prime numbers have received much study, and considerable efforts have been spent trying to determine the nature of their distribution in the sequence of positive integers. The chief results along this line obtained in antiquity are Euclid's proof of the infinitude of primes and Eratosthenes' *sieve* for finding all primes below a given integer n.

Euclid's proof, in Proposition 20 of Book IX of his *Elements*, that *the number of prime numbers is infinite*, has been universally regarded by mathematicians as a model of mathematical elegance. The proof employs the indirect method, or *reductio ad absurdum*, and runs essentially as follows. Suppose there is only a finite number of prime numbers, which we shall denote by $a, b, \cdots, k$. Set $P = a, b, \cdots k$. Then $P + 1$ is either prime or composite. But, since $a, b, \cdots, k$ are all the primes, $P + 1$, which is greater than each of $a, b, \cdots, k$, cannot be a prime. On the other hand, if $P + 1$ is composite, it must be divisible by some prime p. But p must be a member of the set $a, b, \cdots, k$ of all primes, which means that p is a divisor of P. Consequently, p cannot divide $P + 1$, since $p > 1$. Thus our initial hypothesis that the number of primes is finite is untenable, and the theorem is established.

The so-called *sieve of Eratosthenes* is a clever device noted by the Greek mathematician Eratosthenes (*c.* 230 B.C.) for finding all the prime numbers less than a given number n. One writes down, in order and starting with 3, all the odd numbers less than n. The composite numbers in the sequence are then sifted out by crossing off, from 3, every third number, then from the next remaining number, 5, every fifth number, then from the next remaining number, 7, every seventh number, from the next remaining number, 11, every eleventh number and so on. In the process some numbers will be crossed off more than once. All the remaining numbers, along with the number 2, constitute the list of primes less than n.

From the sieve of Eratosthenes can be obtained a cumbersome formula which will determine the number of primes below n when the primes below $\sqrt{n}$ are known. This formula was considerably improved in 1870

* Adapted from Howard Eves, *An Introduction to the History of Mathematics* (New York: Rinehart & Co., Inc., 1953).

tion of the primes is the so-called *prime number theorem*. Suppose we let A_n denote the number of primes below n. The prime number theorem then says that $(A_n \log_e n)/n$ approaches 1 as n becomes larger and larger. In other words A_n/n, called the *density* of the primes among the first n integers, is approximated by $1/\log_e n$, the approximation improving as n increases. This theorem was conjectured by Gauss from an examination of a large table of primes, and was independently proved in 1896 by the French and Belgian mathematicians J. Hadamard and C. J. de la Vallée Poussin.

Extensive factor tables are valuable in researches on prime numbers. Such a table for all numbers up to 24,000 was published by J. H. Rahn in 1659, as an appendix to a book on algebra. In 1668, John Pell, of England, extended this table up to 100,000. As a result of appeals by the German mathematician J. H. Lambert, an extensive and ill-fated table was computed by a Viennese schoolmaster named Felkel. The first volume of Felkel's computations, giving factors of numbers up to 408,000, was published in 1776 at the expense of the Austrian imperial treasury. But there were very few subscribers to the volume, and so the treasury recalled almost the entire edition and converted the paper into cartridges to be used in a war for killing Turks! In the nineteenth century, the combined efforts of Chernac, Burckhardt, Crelle, Glaisher, and the lightning calculator Dase led to a table covering all numbers up to 10,000,000, and published in ten volumes. The greatest achievement of this sort, however, is the table calculated by J. P. Kulik (1773–1863), at the University of Prague. His as yet unpublished manuscript is the result of a 20-year hobby, and covers all numbers up to 100,000,000. The best available factor table is that of the American mathematician D. N. Lehmer (1867–1938). It is a cleverly prepared one-volume table covering numbers up to 10,000,000.

There are many unproved conjectures regarding prime numbers. One of these is to the effect that there are infinitely many pairs of *twin primes*, or primes of the form p and $p + 2$, like 3 and 5, 11 and 13, and 29 and 31. Another is the conjecture made by C. Goldbach in 1742 in a letter to Euler. Goldbach had observed that every even integer, except 2, seemed representable as the sum of two primes. Thus $4 = 2 + 2$, $6 = 3 + 3$, $8 = 5 + 3, \cdots, 16 = 13 + 3, 18 = 11 + 7, \cdots, 48 = 29 + 19, \cdots, 100 = 97 + 3$, and so forth. Progress on this problem was not made until 1931 when the Russian mathematician Schnirelmann showed that every positive integer can be represented as the sum of not more than 300,000 primes! Somewhat later the Russian mathematician Vinogradoff showed that there exists a positive integer N such that any integer $n > N$ can be expressed as the sum of at most four primes, but the proof in no way permits us to appraise the size of N.

FOREWORD

A dramatic device bequeathed by the ancients is the Sieve of Eratosthenes (c. 230 B.C.), who flourished about the time of Apollonius and Archimedes, two of the greatest Greek mathematicians. This is a simple device for testing whether or not a positive integer m is a prime by systematically striking out all composite numbers which precede m. How long must this process of striking out integers be continued before we know that m is a prime? Eratosthenes provided the answer by the following theorem, which thus becomes a useful test for a prime:

> A positive integer m is a prime if it has no positive prime factor less than or equal to I, where I is the greatest integer such that I^2 is less than or equal to m.

The present article not only explains the classical Sieve of Eratosthenes but extends the discussion to modern developments including the so-called *random sieve*, which is then related to the "prime number theorem." This theorem, anticipated by Gauss during the first half of the nineteenth century, was refined and improved by 1900 in the form

$$\lim_{x \to \infty} \left(\frac{\pi(x)}{x/\log x} \right) = 1.$$

It is of interest to note that the famous Russian mathematician Tchebysheff (1821–1894) succeeded in showing that for any real number $n > 3\frac{1}{2}$ there is always at least one prime between n and $2n - 2$.

Mathematical Sieves

They sift out prime numbers and similar series of integers. Recent research into their properties suggests that a kind of uncertainty principle may exist even in pure mathematics

David Hawkins

It is no accident that the theories of probability and statistics are among the most rapidly growing branches of modern mathematics. Science demands them. Faced with problems too complex, or too little understood, to solve exactly, it falls back on laws or facts that are true only probably, or on the average. And from physics, considered the most exact of sciences, we learn that at bottom nature is inescapably uncertain and chancy.

But if we must settle for a gambler's view of the real world, can we not console ourselves with the thought that in the abstract realm of mathematics certainty is always possible? As this article will indicate,

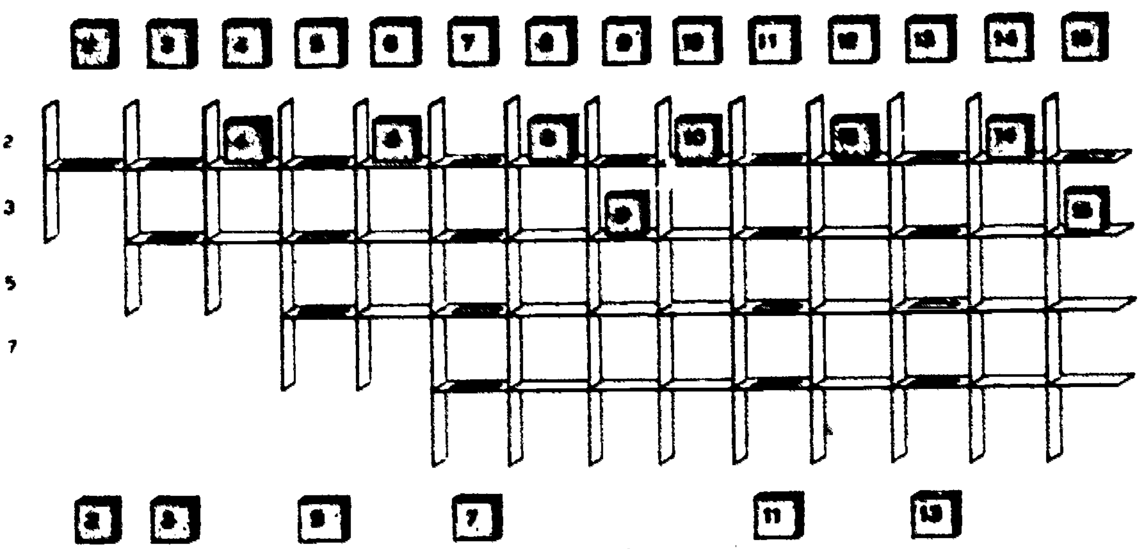


Figure 1

SIEVE OF ERATOSTHENES, a small part of which is shown here, was devised more than 2,000 years ago to separate prime and composite numbers. The first "layer" of the sieve screens out multiples of 2 from the series of integers at the top. Since 3 passes through this layer, it screens out its own multiples in the next layer. Numbers at the bottom are primes which have passed through all previous layers: they will become screening numbers in their turn. No simpler method of deriving primes has yet been devised.

the answer is by no means clear. Some provinces of mathematics are so difficult that, for the present at least, they must make do with rules which are only probably true. Even in mathematics there may be an uncertainty principle not utterly unlike the uncertainty principle of physics.

The text of this sermon derives not from some new and exotic kind of mathematics but from arithmetic. We shall discuss the classical problem of prime numbers. These are the positive integers—2, 3, 5, 7, 11 and so on—which cannot be represented by multiplying two smaller numbers. (Numbers which can be represented by such multiplication —4, 6, 8, 9, 10, 12 and so on—are called composite numbers.) Prime numbers have fascinated mathematicians for centuries. It was Euclid who proved there is an infinite number of them. Since then many brilliant minds have turned to primes and have discovered a number of remarkable theorems concerning them. Even more remarkable is what has not been discovered. For example, what is the 34th prime number? What is the billionth? The *n*th? To this day there is no general formula to answer these questions. The only way to find the billionth prime would be to write down all of the first billion and take the last. As another example, consider the famous twin-prime problem. Pairs of primes such as 11 and 13 or 29 and 31, which are separated by only one other number, are known as twins. They keep turning up in the longest series of primes that have yet been listed. Will they continue to recur indefinitely? Is their number infinite? It seems probable, but no one has been able to prove it.

The study of prime numbers has been quite literally as much an experimental as a theoretical investigation. Most of the facts that have been proved began as conjectures, based on the inspection of an actual series of primes. Many conjectures remain, seeming more or less probably true. Thus an indispensable tool of the number theorist is a long list of primes.

One of the best known, now found in every well-equipped mathematics library, was compiled by D. N. Lehmer of the University of California in 1914. The volume contains a table of the 664,580 prime numbers smaller than 10,000,000, plus a few more to fill the last column, ending with the prime 10,006,721. Lehmer's work was completed before the age of automatic computation; today there are even longer lists, the longest being "published" only on magnetic tape.

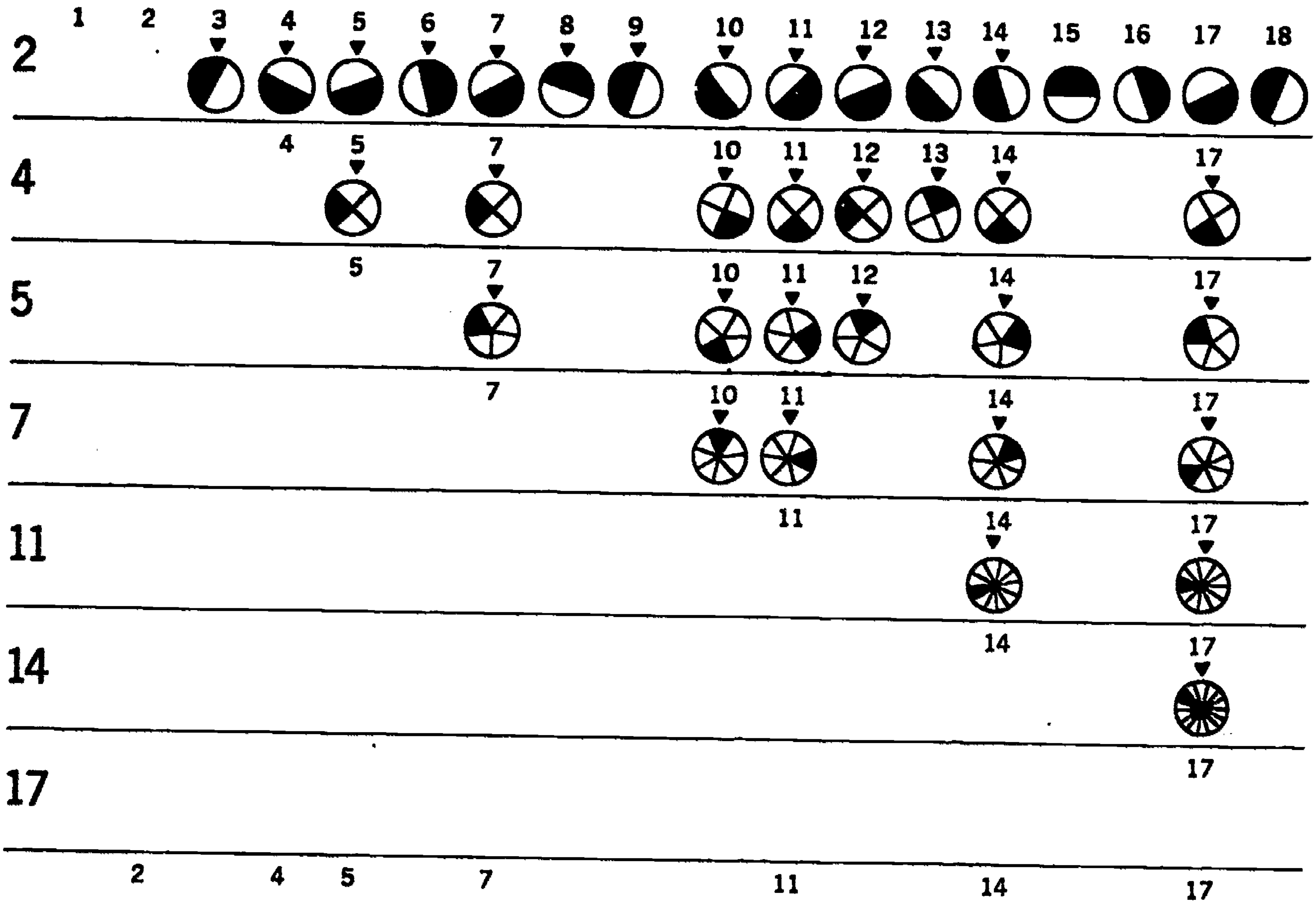
Modern tables of primes are prepared by a method, essentially unaltered for 2000 years, which is called the sieve of Eratosthenes. Its inventor was one of those great figures of the Hellenistic Age who seem today, across the intervening centuries, so clairvoyant of the spirit of modern science. Eratosthenes of Alexandria is best known for his feat

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
2				(2x2)		(2x3)		(2x4)		(2x5)		(2x6)		(2x7)		(2x8)	
3									(3x3)						(3x5)		
5																	
		2	3		5		7				11		13				17

	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
2	(2x9)		(2x10)		(2x11)		(2x12)		(2x13)		(2x14)		(2x15)		(2x16)		(2x17)
3				(3x7)						(3x9)						(3x11)	
5								(5x5)									
		19				23						29		31			

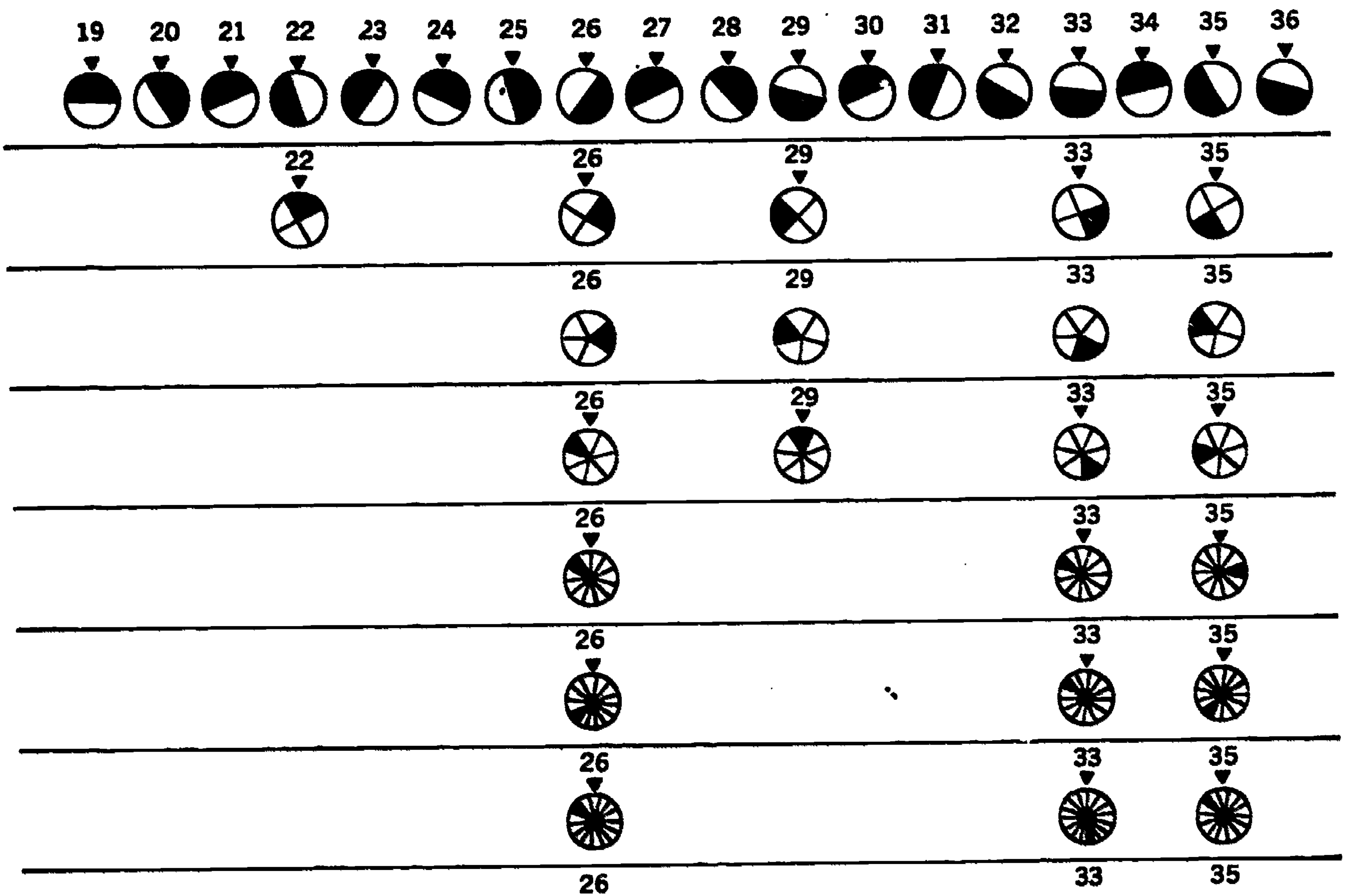
PRIME-NUMBER SIEVE shown here is a larger portion of the sieve shown in FIGURE 1. Primes appear on the bottom line. Each prime in turn becomes a sieving number which eliminates its own multiples, beginning with its square (lower multiples have already been removed by lower primes). Thus each prime eliminates a proportion of the remaining numbers equal to its reciprocal (*e.g.*, 3 removes 1/3, 5 removes 1/5). The steps shown here in part yield all primes up to 49, the square of the next sieving number.

Figure 2



RANDOM-NUMBER SIEVE is statistically similar to the prime sieve but differs from it in detail. In both cases numbers not previously eliminated become seiving numbers; these screen out a proportion of the remaining numbers equal to their reciprocals.

Figure 3a



In the random sieve, however, the specific numbers to be eliminated are chosen by a random process symbolized by the colored wheels. Thus the random sieve produces a different set of numbers each time it is used, while the set of prime numbers is invariant.

Figure 3b

13

of measuring the size of the earth. But he was a man of universal learning who wrote also on geometry, the measurement of time, and the drama. In his own day he was nicknamed "Beta" because, it was said, he stood at least second in every field. Modern electronic computers can make far longer lists of primes than Eratosthenes could have, but his principle of computation has not been much improved.

The method is almost obvious *(see Figure 1)*. Simply write down a series of positive integers and proceed systematically to eliminate all the composite numbers. The numbers that remain—that fall through the "sieve"—are primes. We begin by knocking out the even numbers, which are multiples of the first prime number: 2. (One is not usually called a prime.) When we have done this, the smallest of the remaining numbers is the second prime: 3. Now we eliminate the multiples of 3 from the numbers which survived the first sieving operation. Five is the next number remaining, so its multiples drop out next; then the multiples of 7, and so on.

The reader may wish to try a somewhat longer version of the sieve than the one shown in the illustration, where 7 is the largest sieving number. In number theory the distance from the obvious to the profound is sometimes very short, and any amateur willing to play the game is on the verge of some first-class mysteries. At any rate, a little manipulation of the sieve will make clear some of its properties. Every sieving number is a prime. The first number sieved out by each one is its own square: the first number eliminated by 2 is 4; by 3, 9; by 5, 25 and so on. In addition, the fraction of the remaining integers eliminated by each sieving number is its own reciprocal: 2 sieves out half of the remaining numbers, 3 sieves out a third, 5 sieves out a fifth.

By carrying out the sieving operation through the prime number 31, we can obtain all the primes in the first 1,368 integers. (The first number sieved out by 37, the next prime, is 37^2, or 1,369.) For purposes of illustration we have arranged the first 1,024 of the integers in a 32×32 array, with the prime numbers shown in italics *(see Figure 4)*. The list is short, but it does demonstrate that the frequency of primes slowly decreases in a rather irregular way. From considerably longer tables Adrien Marie Legendre, and later Karl Friedrich Gauss, were able to guess one of the most important facts about primes—the celebrated Prime Number Theorem. This tells how many primes we may expect to find by carrying the list out to any given number. It states that if the number is n, then there are about n divided by the logarithm of n ($n/\log n$) primes before it. As n grows larger, the error in the formula becomes a smaller and smaller proportion of the exact number of primes. Gauss, whose skill in computing belied the myth that mathematicians cannot add and subtract, arrived at the theorem by a combination of

PRIME SERIES

																																Row Total	Cumulative Total
1	**2**	**3**	4	**5**	6	**7**	8	9	10	**11**	12	**13**	14	15	16	**17**	18	**19**	20	21	22	**23**	24	25	26	27	28	**29**	30	**31**	32	11	11
33	34	35	36	**37**	38	39	40	**41**	42	**43**	44	45	46	**47**	48	49	50	51	52	**53**	54	55	56	57	58	**59**	60	**61**	62	63	64	7	18
65	66	**67**	68	69	70	**71**	72	**73**	74	75	76	77	78	**79**	80	81	82	**83**	84	85	86	87	88	**89**	90	91	92	93	94	95	96	6	24
97	98	99	100	**101**	102	**103**	104	105	106	**107**	108	**109**	110	111	112	**113**	114	115	116	117	118	119	120	121	122	123	124	125	126	**127**	128	7	31
129	130	**131**	132	133	134	135	136	**137**	138	**139**	140	141	142	143	144	145	146	147	148	**149**	150	**151**	152	153	154	155	156	**157**	158	159	160	6	37
161	162	**163**	164	165	166	**167**	168	169	170	171	172	**173**	174	175	176	177	178	**179**	180	**181**	182	183	184	185	186	187	188	189	190	**191**	192	6	43
193	194	195	196	**197**	198	**199**	200	201	202	203	204	205	206	207	208	209	210	**211**	212	213	214	215	216	217	218	219	220	221	222	**223**	224	5	48
225	226	**227**	228	**229**	230	231	232	**233**	234	235	236	237	238	**239**	240	**241**	242	243	244	245	246	247	248	249	250	**251**	252	253	254	255	256	6	54
257	258	259	260	261	262	**263**	264	265	266	267	268	**269**	270	**271**	272	273	274	275	276	**277**	278	279	280	**281**	282	**283**	284	285	286	287	288	7	61
289	290	291	292	**293**	294	295	296	297	298	299	300	301	302	303	304	305	306	**307**	308	309	310	**311**	312	**313**	314	315	316	**317**	318	319	320	5	66
321	322	323	324	325	326	327	328	329	330	**331**	332	333	334	335	336	**337**	338	339	340	341	342	343	344	345	346	**347**	348	**349**	350	351	352	4	70
353	354	355	356	357	358	**359**	360	361	362	363	364	365	366	**367**	368	369	370	371	372	**373**	374	375	376	377	378	**379**	380	381	382	**383**	384	6	76
385	386	387	388	**389**	390	391	392	393	394	395	396	**397**	398	399	400	**401**	402	403	404	405	406	407	408	**409**	410	411	412	413	414	415	416	4	80
417	418	**419**	420	**421**	422	423	424	425	426	427	428	429	430	**431**	432	**433**	434	435	436	437	438	**439**	440	441	442	**443**	444	445	446	447	448	6	86
449	450	451	452	453	454	455	456	**457**	458	459	460	**461**	462	**463**	464	465	466	**467**	468	469	470	471	472	473	474	475	476	477	478	**479**	480	6	92
481	482	483	484	485	486	**487**	488	489	490	**491**	492	493	494	495	496	497	498	**499**	500	501	502	**503**	504	505	506	507	508	**509**	510	511	512	5	97
513	514	515	516	517	518	519	520	**521**	522	**523**	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	**541**	542	543	544	3	100
545	546	**547**	548	549	550	551	552	553	554	555	556	**557**	558	559	560	561	562	**563**	564	565	566	567	568	**569**	570	**571**	572	573	574	575	576	5	105
577	578	579	580	581	582	583	584	585	586	**587**	588	589	590	591	592	**593**	594	595	596	597	598	**599**	600	**601**	602	603	604	605	606	**607**	608	6	111
609	610	611	612	**613**	614	615	616	**617**	618	**619**	620	621	622	623	624	625	626	627	628	629	630	**631**	632	633	634	635	636	637	638	639	640	4	115
641	642	**643**	644	645	646	**647**	648	649	650	651	652	**653**	654	655	656	657	658	**659**	660	**661**	662	663	664	665	666	667	668	669	670	671	672	6	121
673	674	675	676	**677**	678	679	680	681	682	**683**	684	685	686	687	688	689	690	**691**	692	693	694	695	696	697	698	699	700	**701**	702	703	704	5	126
705	706	707	708	**709**	710	711	712	713	714	715	716	717	718	**719**	720	721	722	723	724	725	726	**727**	728	729	730	731	732	**733**	734	735	736	4	130
737	738	**739**	740	741	742	**743**	744	745	746	747	748	749	750	**751**	752	753	754	755	756	**757**	758	759	760	**761**	762	763	764	765	766	767	768	5	135
769	770	771	772	**773**	774	775	776	777	778	779	780	781	782	783	784	785	786	**787**	788	789	790	791	792	793	794	795	796	**797**	798	799	800	4	139
801	802	803	804	805	806	807	808	**809**	810	**811**	812	813	814	815	816	817	818	819	820	**821**	822	**823**	824	825	826	**827**	828	**829**	830	831	832	6	145
833	834	835	836	837	838	**839**	840	841	842	843	844	845	846	847	848	849	850	851	852	**853**	854	855	856	**857**	858	**859**	860	861	862	**863**	864	5	150
865	866	867	868	869	870	871	872	873	874	875	876	**877**	878	879	880	**881**	882	**883**	884	885	886	**887**	888	889	890	891	892	893	894	895	896	4	154
897	898	899	900	901	902	903	904	905	906	**907**	908	909	910	**911**	912	913	914	915	916	917	918	**919**	920	921	922	923	924	925	926	927	928	3	157
929	930	931	932	933	934	935	936	**937**	938	939	940	**941**	942	943	944	945	946	**947**	948	949	950	951	952	**953**	954	955	956	957	958	959	960	5	162
961	962	963	964	965	966	**967**	968	969	970	**971**	972	973	974	975	976	**977**	978	979	980	981	982	**983**	984	985	986	987	988	989	990	**991**	992	5	167
993	994	995	996	**997**	998	999	1,000	1,001	1,002	1,003	1,004	1,005	1,006	1,007	1,008	**1,009**	1,010	1,011	1,012	**1,013**	1,014	1,015	1,016	1,017	1,018	**1,019**	1,020	**1,021**	1,022	1,023	1,024	5	172

DISTRIBUTION of random "primes" between 1 and 1,024 *(Figure 5)* resembles that of true primes in the same number sequence *(Figure 4)*. Both sets of numbers *(in bold face)* thin out irregularly as the sequence progresses *(see totals at right)*. Another "run" of the random sieve might yield an even more similar distribution. The resemblance of the two series tends to intensify as they are increased in length.

Figure 4

RANDOM SERIES

																																Row Total	Cumulative Total
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	8	8
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	6	14
65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	7	21
97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	8	29
129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	7	36
161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	6	42
193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	4	46
225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	4	50
257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	7	57
289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	6	63
321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	3	66
353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	4	70
385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	3	73
417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	5	78
449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	4	82
481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	3	85
513	514	515	516	517	518	519	520	521	522	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	3	88
545	546	547	548	549	550	551	552	553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571	572	573	574	575	576	4	92
577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593	594	595	596	597	598	599	600	601	602	603	604	605	606	607	608	3	95
609	610	611	612	613	614	615	616	617	618	619	620	621	622	623	624	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	8	103
641	642	643	644	645	646	647	648	649	650	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	3	106
673	674	675	676	677	678	679	680	681	682	683	684	685	686	687	688	689	690	691	692	693	694	695	696	697	698	699	700	701	702	703	704	4	110
705	706	707	708	709	710	711	712	713	714	715	716	717	718	719	720	721	722	723	724	725	726	727	728	729	730	731	732	733	734	735	736	5	115
737	738	739	740	741	742	743	744	745	746	747	748	749	750	751	752	753	754	755	756	757	758	759	760	761	762	763	764	765	766	767	768	5	120
769	770	771	772	773	774	775	776	777	778	779	780	781	782	783	784	785	786	787	788	789	790	791	792	793	794	795	796	797	798	799	800	4	124
801	802	803	804	805	806	807	808	809	810	811	812	813	814	815	816	817	818	819	820	821	822	823	824	825	826	827	828	829	830	831	832	3	127
833	834	835	836	837	838	839	840	841	842	843	844	845	846	847	848	849	850	851	852	853	854	855	856	857	858	859	860	861	862	863	864	5	132
865	866	867	868	869	870	871	872	873	874	875	876	877	878	879	880	881	882	883	884	885	886	887	888	889	890	891	892	893	894	895	896	3	135
897	898	899	900	901	902	903	904	905	906	907	908	909	910	911	912	913	914	915	916	917	918	919	920	921	922	923	924	925	926	927	928	0	135
929	930	931	932	933	934	935	936	937	938	939	940	941	942	943	944	945	946	947	948	949	950	951	952	953	954	955	956	957	958	959	960	1	136
961	962	963	964	965	966	967	968	969	970	971	972	973	974	975	976	977	978	979	980	981	982	983	984	985	986	987	988	989	990	991	992	5	141
993	994	995	996	997	998	999	1,000	1,001	1,002	1,003	1,004	1,005	1,006	1,007	1,008	1,009	1,010	1,011	1,012	1,013	1,014	1,015	1,016	1,017	1,018	1,019	1,020	1,021	1,022	1,023	1,024	4	145

Figure 5

arithmetical insight and purely empirical study. It was not proved for almost another century. In the 1890s the Belgian mathematician Charles de la Vallée Poussin and the French mathematician Jacques Hadamard independently found a proof, but it made use of concepts outside simple whole numbers. It was not until 1950 that the Norwegian mathematician Atle Selberg discovered a purely arithmetical proof. In the quaint vocabulary of number theory his proof is called elementary, but it is not easy.

The difficulties of the Prime Number Theorem are connected with the puzzlingly irregular way in which the primes are distributed. Indeed, the theorem itself does no more than state a statistical average. Outrageous as it may seem, the sequence of primes is just as "random" as many of the natural phenomena on which we make bets. Sometimes we think that if we knew enough about the individual events of which such phenomena are composed, we could predict their outcome with certainty. This is surely true of the primes. The sieve will eventually tell us about the primality of any given number. But it cannot tell us about all numbers, because the sequence is itself an infinite, unending process.

From the time of Gauss mathematicians have talked, perhaps rather shamefacedly, about the "probable" behavior of primes, and this kind of reasoning has been very helpful. No mathematician, however, seems to have gone the whole way and made a purely statistical model of the prime-number distribution. Recently I was led to try it, and I found that the model helps clarify the Prime Number Theorem. Furthermore, it places the whole subject in a new perspective. In particular, the theorem no longer appears as a special fact about the sequence of numbers which cannot be produced by multiplying two smaller numbers, but rather as a common feature of all sequences of numbers generated by sieves of a certain type.

The model is called the random sieve, and it works like this *(see Figure 5)*. Start with 2 as the first sieving number, just as in the method of Eratosthenes. Now make a kind of roulette wheel that is divided into two equal parts, black and white. Go down the list of integers following 2, and for each one spin the wheel. If the black part of the wheel stops at the pointer, strike the integer out; if white stops at the pointer, leave the integer in. Note what you have accomplished. In the long run you will have sieved out half of the integers, just as the first step in the prime number sieve does. But just which ones go out is a matter of chance, and the list will be different each time you try it.

Next take the first number that was not removed. Suppose it was 4. Make a new wheel of which a fourth is black and three-fourths is white. Spin the wheel for each succeeding number left after the first sieving. When black comes up, strike the number out; when white comes up, leave the number in. This time you have removed a fourth of the remaining numbers. Proceed again to the first number not removed — say 5. Repeat the procedure using a sieving probability of $\frac{1}{5}$, and so on. After any number of steps you will be left with a series of integers which might be called "random primes."

If you want to try the sieve yourself, you need not actually make roulette wheels. A table of random numbers or, failing that, a telephone book will do. Express each sieving probability as a four-digit decimal (*e.g.*, $\frac{1}{4} = .2500$). For each "spin of the wheel" read successive telephone numbers. If your probability is $\frac{1}{4}$, then any number whose last four digits are 2499 or less tells you to eliminate the integer in question; 2500 or more means to leave it in.

One run of the random sieve for the first 1,024 integers is summarized in the table on the preceding two pages. Comparing the distribution of these random primes with the actual ones, we can see that our sieve acts something like the sieve of Eratosthenes. This is partly in spite of the random element, but partly because of it. For a much longer series the general statistical similarity would be even closer.

It may seem paradoxical that we can take a statistical model, involving an infinity of random choices, as *ersatz* for the straightforward and perfectly defined sieve of Eratosthenes. The paradox is the same as the one which underlies statistical mechanics: the average behavior of an assembly of molecules is easier to describe than the actual behavior of any one of them. Of course the random sieve preserves only the general features of the prime-number sieve. The eccentricities of the latter are averaged out by randomizing them. In either case any number not sieved out becomes in turn a sieving number. It starts a process by which a proportion of later numbers is removed, equal to the reciprocal of that sieving number. Every wave of sieving in the prime-number sieve, except the first, is determined strictly by the result of previous waves. At every corresponding point the random sieve makes probability choices, partly determined by its own earlier statistical behavior.

How closely the random sieve actually approximates the sieve of Eratosthenes is demonstrated by the fact that the Prime Number Theorem holds for random primes. This can be proved by some elementary mathematics, which in this case is also fairly easy *(see Figure 6)*.

Perhaps the parallel between the two sieves is not so surprising. We might say, indeed, that the prime-number sieve would have to be remarkably abnormal in its detailed behavior not to lead to the same general result as the random sieve. This statement implies that the random sieve can be taken as a criterion of normality.

If so, there must be other sieves — in fact, an infinite number of other sieves — that have the same general characteristics as those of the sieve of Eratosthenes, but which differ somewhat in the details of their definition. They will not yield the prime numbers in general, but numbers having some other special property. In 1956, as it happens, Stanislas M. Ulam and his associates at the Los Alamos Scientific Laboratory published some results of a new type of sieve which yields what they called "lucky" numbers. Their sieve begins by removing the multiples of 2, leaving 3 as the first number not sieved out. Instead of removing next the multiples of 3, the Ulam sieve removes every third remaining number. Since 5 is the third number in the list of remaining numbers, it drops out, but 7 remains. Hence in the next wave every seventh number of those still remaining is eliminated, and so on *(see Figure 8)*. The numbers that escape are "lucky." It has been proved that the analogue of the Prime Number Theorem holds for lucky numbers. Thus the random sieve is a model for the lucky numbers as well as for the primes.

So far the random sieve has only duplicated results that can be obtained independently and rigorously for the sieves of Eratosthenes and of Ulam. The mathematics of it, however, is mostly easier. Therefore many additional theorems can be obtained from the random sieve and conjectured to be true of the other two. Such conjectures are not proofs, but we can say that unless the prime number and lucky sieves are vastly abnormal, the results must hold for them.

Let us look at a couple of examples. As we go to larger and larger numbers in the table of integers, the spacing between successive primes (or luckies or random primes) grows greater in an irregular way. In the neighborhood of any number, n, the average interval is about the logarithm of n. What is the greatest interval? We do not know the answer for primes or luckies. But for the random sieve we can prove that, with only a finite number of exceptions, the interval is never greater than the square of the logarithm of n, that is, $(\log n)^2$. The chance that there will be any further exceptions can be made as small as we please by taking a sufficiently large n. No upper boundary to the interval between successive primes or successive luckies has been found which is anywhere nearly as small, although from the existing tables it looks as though the formula should hold for them too.

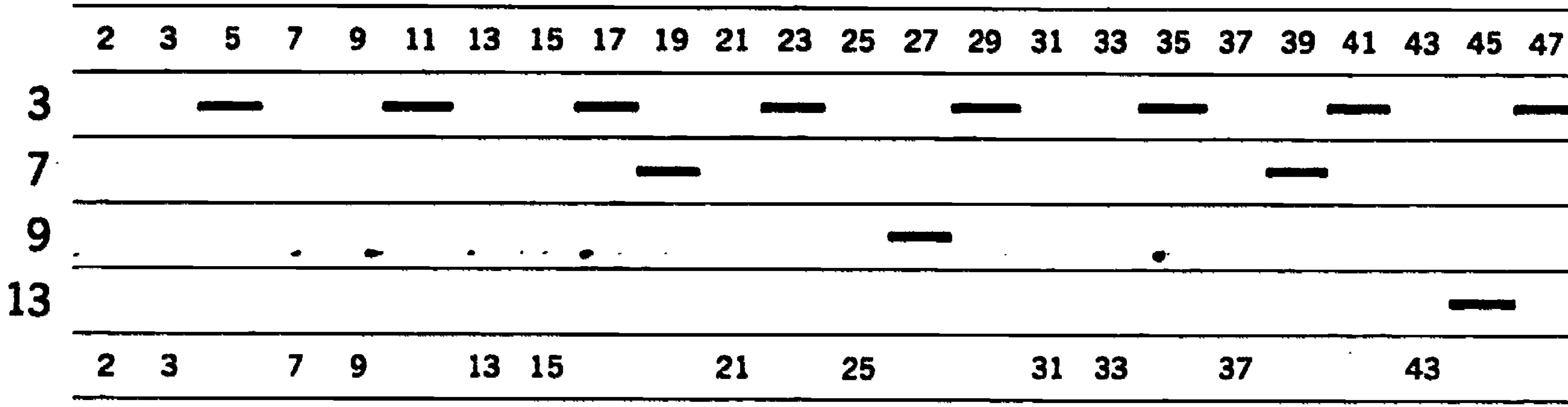
Another example is the twin-prime problem mentioned earlier. In the random sieve there is almost certainly an infinite number of twins. Indeed the average interval between twins ought to be about $(\log n)^2$, and the maximum interval between them, with only a finite number of exceptions, ought to be $(\log n)^3$. Again the tables suggest that these results are also true for primes and luckies, but no one has any idea how to prove such results.

Although the random sieve does not solve any classical problems concerning primes, it does enable us to reformulate such problems. We may ask: "Are the prime numbers normal in such and such a respect?"

The random sieve, or certain modifications of it, defines what we mean by normality. If the properties we are talking about depend on the exact fine structure of the sequence of primes, the answer will obviously be no. Thus all primes except the number 2 are odd, while this is infinitely improbable in the sequences of random primes. But average properties such as those we have discussed do not seem to depend on the fine structure, and those may be presumed to be normal for primes or luckies. Can anyone find a major abnormal property, in this sense, of the sequence of primes? Or the sequence of luckies?

In the opinion of the author the concept of normality raises some very deep questions about numbers and the theory of numbers. Sieves as a class are a type of feedback mechanism: the output of one stage of the process determines the input of the next stage. Now in any such mechanism the nature of the coupling between output and input is crucial; the result may be stable and predictable for one type of coupling and unstable for another. So far as the outcome of the random sieve is concerned, it is in one respect extremely stable. If by chance there are relatively few sieving numbers in the early stages, they will remove relatively few later on, and so there will be an increase in the later stages to compensate for the initial deficit. The sieves of primes and luckies share this characteristic. But this is a statistical stability.

When we look at other aspects of the prime or the lucky sieve, however, we find elements of instability. The detailed ordering of primes or luckies depends upon the individual sieving numbers that precede them, and this involves a growth of complexity without apparent limit. Some easily defined properties of normal sequences, for example the two described, may depend strongly enough on this complexity to make it impossible, in a finite number of steps, to prove that they hold. Here is the analogy, if it be one, with the uncertainty principle of physics: An infinite complexity requires infinite time to resolve it. If our suggestions have substance, we will have examples of mathematical statements which are almost certain, but which cannot, in principle, be proved. Examples of undecidable propositions are known in modern arithmetic [see "Gödel's Proof," by Ernest Nagel and James R. Newman; SCIENTIFIC AMERICAN, June, 1956], but so far none of the unproved conjectures about prime numbers has been shown to be undecidable. Perhaps none of them is. If any are, however, the random sieve will be a model for the primes in a deeper sense than any we have exploited in this article. We cannot distinguish an infinitely complex order from a random one, and so we might be forced to admit that there is a certain background of noise even among the eternal verities.



"LUCKY" NUMBER SIEVE resembles the prime and random sieves already described. Here, also, numbers which are not eliminated become sieving numbers and remove a proportion of the remaining numbers equal to their reciprocals. Elimination is by counting: thus 3 removes every third remaining number, 7 every seventh. Like primes, the "lucky" numbers form an invariant series.

Figure 8

2	3	7	9	13	15	21	25	31 ★ 33	37	43	49	51	63 ★ 67	69	73	75	79	87	93 ★ 99
105	111	115	127 ★ 129	133	135	141	151	159 ★ 163	169	171	189 ★ 193	195	201	205	211	219	223 ★ 231	235	
237	241 ★ 259	261	267	273	283	285 ★ 289	297	303	307	319 ★ 321	327	331	339	349 ★ 357	361	367 ★ 385	391		
393	399	409	415 ★ 421	427	429	433 ★ 451	463	475	477 ★ [illegible]	487	489	495	511 ★ 517	519	529	535	537	541★	
553	559 ★ 577	579	583	591	601 ★ 613	615	619	621	631	639 ★ 643	645	651	655 ★ 673	679	685	693	699 ★ 717		
723	727	729	735 ★ 739	741	745 ★ 769	777	781	787 ★ 801	805	819	823	831 ★ 841	855 ★ 867	873	883	885	895★		
897	903	925	927 ★ 931	933	937	957 ★ 961	975	979	981	991 ★ 993	997	1009	1011	1021	1023 ★				

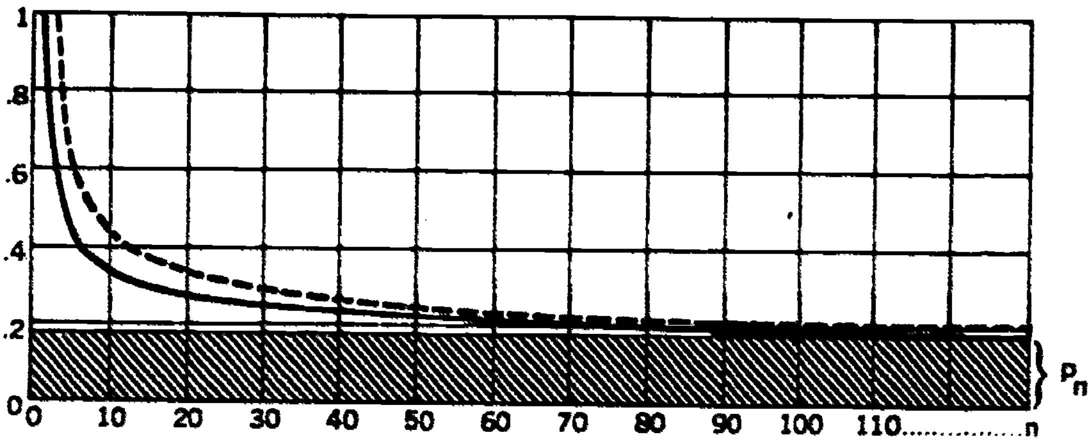
DISTRIBUTION OF "LUCKY" numbers between 1 and 1,024 resembles that of primes and random primes, thinning out gradually but irregularly as the list increases. This table shows only the "luckies"; the intervening numbers are omitted. Stars set off luckies within successive series of 32 integers: each of these groups corresponds to a single line of the tables in Figures 4 and 5.

Figure 9

DERIVATION OF THE PRIME NUMBER THEOREM FOR THE RANDOM SIEVE

Let us consider the fate of any two consecutive numbers, say 127 and 128, on a run through the random-sieving operation. We shall compare their probabilities of getting through the sieve; *i.e.*, of becoming sieving numbers or "random primes" themselves.

Call these probabilities P_{127} and P_{128}. Now it is obvious that 128 runs the same risk of being eliminated by previous sieving numbers as does 127, except for one possibility. If 127 becomes a sieving number, it can eliminate 128, but not *vice versa*. The probability that 127 is a sieving number is P_{127}. If it is a sieving number, the probability that it will eliminate 128 (or any other following number) is 1/127. The chance that the two events will occur and that 127 will eliminate 128 is the product of their probabilities: $P_{127} \times 1/127$. The probability that this will not happen is $1 - P_{127}/127$. Except for this factor the chance of survival for



AVERAGE NUMBER OF RANDOM "PRIMES" in the first n integers is shown by the area under the solid curve, roughly approximated by the hatched rectangle (drawn here for $n = 130$). The area under the broken curve gives the approximate number of true primes. Since the two curves approach each other as n increases, the two sets of primes are very like.

Figure 7

128 is the same as that for 127. Its net probability is therefore the product of the two: $P_{128} = P_{127}(1 - P_{127}/127)$.

At this point it will be more convenient to shift from the probabilities to their reciprocals. The reciprocal of a probability has itself a clear statistical meaning: it gives the average interval, or range, between two events. (Instead of saying that the probability of double six in dice is

1/36, we can as well say that the average interval between throws of double six is 36.) Denote the reciprocal of P_{127} by X_{127}, and of P_{128} by X_{128}. X_{127} measures the average interval between sieving numbers in the neighborhood of 127 and X_{128} measures the same interval in the slightly shifted neighborhood of 128.

By a little algebra we can show that if $P_{128} = P_{127}(1 - P_{127}/127)$, then $X_{128} = X_{127} + 1/127 + r$, where r is a negligibly small remainder. For practical purposes we can say that $X_{128} = X_{127} + 1/127$. Now a similar argument would show that $X_{127} = X_{126} + 1/126$, and so on. Eventually we arrive at the result that $X_{128} = 1 + 1/2 + 1/3 + 1/4 \ldots + 1/127$, or, in general, $X_n = 1 + 1/2 + 1/3 + 1/4 \ldots + 1/n$, with a remainder that is still negligibly small. In calculus books we discover that the series $1 + 1/2 + 1/3 + 1/4 \ldots + 1/n$ is nearly equal to $\log n$ for fairly long series. The difference can be made as small as we like by making n large enough. Therefore we can say that, in the long run, $X_n = \log n$, or $P_n = 1/\log n$.

The graph on the preceding page shows the values of $1/\log n$ (and, for comparison, the reciprocal of the actual values of the series $1 + 1/2 + 1/3 + 1/4 \ldots + 1/n$). Thus the curve is also a graph of P_n. Suppose we now want to know how many random primes, on the average, there should be before any number n. We simply add the probabilities that each smaller number becomes a sieving number. Graphically this is the same as taking the area under the curve. But if n is very large, then the difference between the area under the curve and the area of the shaded rectangle, which is $n \times P_n$ is negligible. Hence we can say that the average number of random primes out to n is $n \times P_n$. But $P_n = 1/\log n$, so the number becomes $n/\log n$. And this is the Prime Number Theorem!

Having completed the proof, we may reexamine our reasoning to see why the result is plausible. The essential step was to find that $X_n + 1 = X_n + 1/n$. This equation says that on the average, over many repetitions of the sieve, any number n removes enough of the numbers following to lengthen the interval between them by $1/n$. Take a specific example. Suppose that P_{127} is 1/5 and X_{127} is 5. Then 127 will be a sieving number 1/5 of the time. When it is, it will eliminate about 1/127 of the remaining numbers, lengthening the average interval between them from 5 to $5 + 5/127$. Since it only does this about one time out of every five trials of the sieve, its average effect will be to lengthen the interval from 5 to $5 + 1/127$.

The same chain of reasoning is plausible for the prime-number sieve.

FOREWORD

You have already seen how the Sieve of Eratosthenes can be used to determine all the primes up to any desired number. In the present essay we find an ingenious modification of the sieve in the form of a mechanical chart, which reveals additional properties of the primes.

The property of greatest interest, perhaps, is the fact that any prime greater than 3 is equal either to one more or one less than a multiple of 6. Although the author proves this property, you might like to refer to a table of primes and verify this property for a few cases.

The Factorgram[1]

Kenneth P. Swallow

The problem of finding all the prime numbers has intrigued mathematicians through the ages. The many attempts to solve this problem have yielded only methods that will produce a finite number of primes, the most noted of these being the Sieve of Eratosthenes. The Factorgram is an adaptation of this systematic mechanical method.

In the Eratosthenes Sieve, to find all the primes less than a selected number, N, all the integers from 2 to N are written in order. The number 2, which is known to be a prime, is encircled and every second number from 2 is crossed out. These are the multiples of 2 and hence cannot be primes.

2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~	11
~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~	etc.

The number 3, which is prime because it is the only remaining number less than 2^2, is encircled and every third number from 3 is crossed out.

2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11
~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~	etc.

Now, 5 and 7 are the only remaining numbers less than 3^2, therefore they must be prime numbers. This process is continued until every multiple of every prime number up to $\sqrt{N}$ is crossed out. The remaining numbers are the prime numbers less than N.

HOW TO MAKE A FACTORGRAM

To find all the prime numbers less than a selected number, N, by the Factorgram, place all the numbers from 0 to N in rows of six numbers as follows:

0	1	2	3	4	5
6	7	8	9	10	11
12	13	14	15	16	17
18	19	20	21	22	23
24	25	26	27	28	29
30	31	32	33	34	35
36	37	38	39	40	41

Now the multiples of 2 can be crossed out by drawing lines through the entire first, third and fifth columns, with the exception of the number 2 itself. Similarly, the multiples of 3 can be crossed out by drawing a line

[1] Kenneth P. Swallow, "Elementary Number Theory in High School Mathematics," pp. 84-93. Unpublished Master's Thesis, Ohio State University, 1952.

through the entire fourth column, with the exception of the number 3 itself. The first column contains multiples of 3 but it is already crossed out. Next, the multiples of 5 are to be crossed out. The first six of these, 5, 10, 15, 20, 25, and 30, lie in a straight line running diagonally downward from right to left. The next six multiples of five (35 to 60) lie in another straight line, which is parallel to the first line. All the multiples of 5 can be crossed out by a set of such parallel lines. Next, the multiples of 7 can be crossed out by a set of such parallel lines running downward from left to right. The multiples of all prime numbers can be crossed out by similar sets of parallel lines. In the Factorgram as in the Eratosthenes Sieve, when all the multiples of all the prime numbers less than $\sqrt{N}$ are crossed out the remaining numbers less than N are all primes.

The Factorgram can be made on a piece of paper and then rolled into a cylinder so that the numbers form a helical spiral. (In Figure 1, roll so that the two zeros coincide.) In this form, each of the sets of parallel lines which cross out the multiples of the prime numbers will also form a helical spiral.

FEATURES OF THE FACTORGRAM

The main purpose of the Factorgram, as of the Eratosthenes Sieve, is to find all the primes up to any selected number. However, the Factorgram has many features not found in the usual Sieve.

1. The mechanical process is very easy. The columns of numbers can be made quickly with a typewriter. If a long Factorgram is to be made, periods should be placed after the numbers as was done in Figure 1. The period, rather than the figure, is used to represent the exact location of each number. (In Figure 1 the distance from the zero line to each number is proportional to the magnitude of the number. This improves the Factorgram in its cylindrical form but is not really necessary for proper operation.) A pair of draftsman's triangles can be used to draw the parallel lines needed to cross out the multiples of each prime number. The first line of each set of parallel lines is determined by zero and the prime number. All such lines pass through zero, since zero is a multiple of every number.

2. The prime numbers, which seem to be so haphazardly scattered through the number system have, with the exception of 2 and 3, settled down to occupy positions in only two of the Factorgram's six columns.

3. The presence of prime pairs of the form p and $p + 2$, such as 5 and 7, 11 and 13, etc., and of the form p and $p + 4$, such as 7 and 11, 13 and 17, etc., become more obvious. Also, the relationships of prime numbers to the number 6 are emphasized.

4. Just as a prime number can be identified by the lack of lines pass-

ing through it, a composite number can be identified by the one or more lines passing through it. These lines provide a means, free of all trial-and-error methods, for finding all the prime factors of a composite number. It is this property of the Factorgram which gives it its name.

The method of factoring a composite number by the Factorgram is as follows: First locate the number on the Factorgram and trace any one of the lines passing through it back to its prime number origin (the last number on the line before reaching zero). This number is one of the prime factors of the original composite number. Divide the original number by this prime factor to obtain a second factor. Find this new factor on the Factorgram to see whether it is prime or composite. If it is prime, the problem is completed; if it is composite, continue the process until the factors of this factor are prime.

For a numerical example, consider the factoring of 117. There are two lines passing through it on the Factorgram. One of these goes back to 3. Dividing 117 by 3 we have 39. On the Factorgram, 39 has two lines passing through it also, one going to 3 and the other to 13. Therefore, the factors of 117 are $3 \cdot 3 \cdot 13$.

Frequently the divisions will be unnecessary because there may be as many lines passing through the given number as there are prime factors of the number. In this case, each line will give one of the prime factors. In fact, the necessity for division occurs only in two cases, (a) if the same number occurs as a factor two or more times, and (b) if one of the factors is greater than the square root of the largest number on the Factorgram. Variations of the Factorgram that will eliminate the division in both of these cases can be made but these variations become overly complicated with too many lines.

5. If two numbers have a common factor, they will be connected on the Factorgram by the line representing that factor. For example, 26 and 65 are connected by the line that passes through 13; 88 and 121 are connected by the line that passes through 11; and 70 and 105 are connected by two lines, one passing through 5 and the other passing through 7. This property of the Factorgram can be useful in reducing fractions. By locating the numerator and the denominator of a fraction, one can tell whether the fraction can be reduced and if so, by what number the numerator and denominator should be divided.

WHY THE FACTORGRAM WORKS

The unusual properties of the Factorgram are based entirely upon the following proposition:

Theorem: All prime numbers greater than 3 are either one more or one less than a multiple of 6.[2]

In other words, all primes greater than 3 are given by one of the two

3!

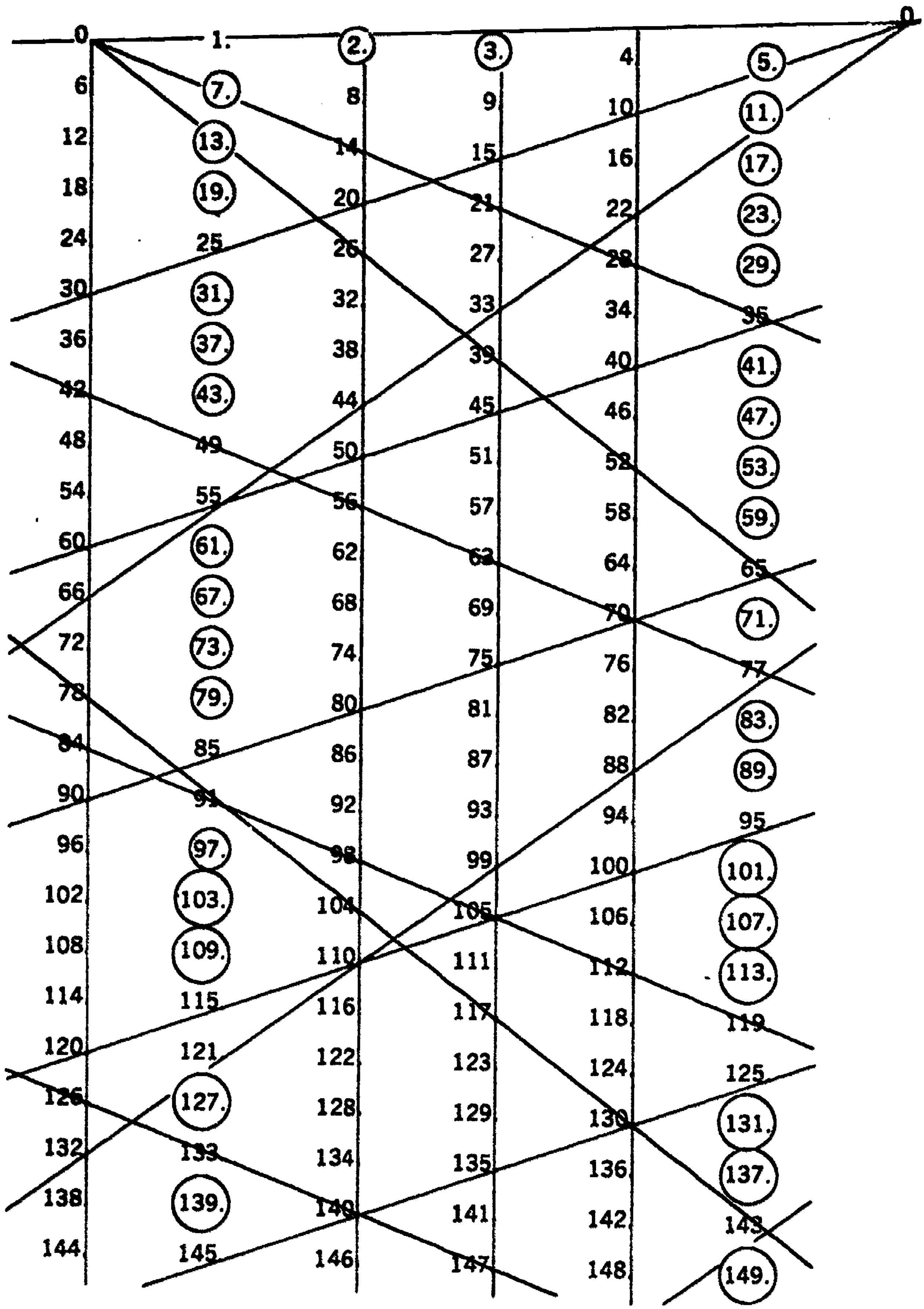


Figure 1. THE FACTORGRAM
(1 to 149)

expressions, $6n + 1$ or $6n - 1$. For example, $6(1) + 1 = 7$, $6(2) + 1 = 13$ and $6(3) + 1 = 19$, while $6(1) - 1 = 5$, $6(2) - 1 = 11$, and $6(3) - 1 = 17$. Of course, the converse of this statement is not necessarily true. For many values of n, the expressions $6n + 1$ and $6n - 1$ will not yield primes; for example, $n = 4$ in $6n + 1$ gives 25, $n = 6$ in $6n - 1$ gives 35, and $n = 8$ in $6n + 1$ gives 49.

The proof of this theorem is quite simple. Every number can be expressed by one of the following six forms, four of which are always factorable, if n is greater than zero.

$6n$	$= 6(n)$
$6n + 1$	not factorable
$6n + 2$	$= 2(3n + 1)$
$6n + 3$	$= 3(2n + 1)$
$6n + 4$	$= 2(3n + 2)$
$6n + 5$ (or $6n - 1$)	not factorable

The expressions $6n + 5$ and $6(n + 1) - 1$ are equivalent since 5 more than a multiple of 6 is also 1 less than the next multiple of 6. Obviously, if four of these six expressions are always factorable, the primes must be expressed by the other two expressions, and hence, the theorem is true.

Now, in the Factorgram, n is the number of each row (if the first row is 0), and the six columns are, from left to right, $6n$, $6n + 1$, $6n + 2$, $6n + 3$, $6n + 4$, and $6n + 5$.

n	$6n$	$6n + 1$	$6n + 2$	$6n + 3$	$6n + 4$	$6n + 5$
0	0	1	2	3	4	5
1	6	7	8	9	10	11
2	12	13	14	15	16	17
3	•	•	•	•	•	•

Therefore, from the above theorem, all the prime numbers above 3 must lie in the second and fifth columns.

The multiples of a prime of the form $6n + 1$ must be $2(6n + 1)$, $3(6n + 1)$, $4(6n + 1)$, etc. These, when simplified are $12n + 2$, $18n + 3$, $24n + 4$, etc., or $6n' + 2$, $6n'' + 3$, $6n''' + 4$, etc. Hence, the multiples of $6n + 1$ must progress in regular fashion from the second column to the third column, the third to the fourth, the fourth to the fifth, and so on. In a similar manner, the multiples of a prime of the form $6n - 1$

[1] In congruence notation, for $p > 3$, for $p \equiv \pm 1 \pmod 6$.

(the same as $6n + 5$) progress from one column to the next, but in this case they progress from right to left.

The number of rows the line passing through the multiples of a prime goes down as it progresses forward or backward from one column to the next is given by the value of n for that prime. For example, the line through the multiples of 7, for which $n = 1$ in $6n + 1$, goes down one row as it progresses forward one column, while the line passing through the multiples of 19, for which $n = 3$ in $6n + 1$, goes down three rows as it progresses forward one column. If the prime is of the form $6n - 1$ the line passing through its multiples will progress backward (right to left) instead of forward.

This sort of slope is helpful both in setting up the parallel lines in making the Factorgram and in using the Factorgram in factoring. In a long Factorgram it is not necessary to trace the parallel lines or spirals back to the prime that produced them. One merely needs to locate the number to be factored and note how many rows down the line (or lines) goes as it progresses forward or backward one column. This number is the value of n which is to be substituted in $6n + 1$ if it progresses forward or $6n - 1$ if it progresses backward. The value of the resulting expression is the same prime number that would be obtained if the line were traced back to its origin.

While the Factorgram is neither particularly profound nor useful, it is simple enough for high school students to understand and offers many opportunities for interesting classroom or mathematics club discussion as do the Eratosthenes' Sieve, Pascal's Triangle, and Magic Squares.

FOREWORD

Consider the factors of the integer 6, namely, 1, 2, 3, and 6; their sum is 12, or twice 6. Again, the factors of 28 are 1, 2, 4, 7, 14, and 28; their sum is 56, or twice 28. Such numbers are called *perfect numbers*. An integer is said to be a perfect number if the sum of its factors is twice the given integer. A perfect number is also defined as any integer which equals the sum of its proper factors, where a "proper" factor of a number means any of its divisors except the number itself.

The ancient Greeks were familiar with perfect numbers. In fact, Euclid proved that if an even integer is of the form

$$2^{p-1} \cdot (2^p - 1), \text{ where } 2^p - 1 \text{ is a prime,}$$

then that integer is a perfect number.

The converse theorem was proved by Euler some two thousand years later. If an integer is an even perfect number, it has the form

$$2^{p-1} \cdot (2^p - 1), \text{ where both p and } 2^p - 1 \text{ are primes.}$$

It is interesting to note that all known perfect numbers are even. Although no odd perfect number has ever been found, mathematicians have not yet succeeded in proving that none exists.

Integers of the form $2^p - 1$, where p is a prime, are called Mersenne numbers, after the French mathematician Marin Mersenne (c. 1620). They play an important role in the study of perfect numbers. Mersenne numbers are designated as $M_p = 2^p - 1$, where p is a prime. Thus, for $p = 5$, $M_5 = 2^5 - 1 = 31$. If M_p is a prime number, it is called a Mersenne prime. Until recently, only 20 Mersenne primes were known. In 1963 the three largest known Mersenne primes, M_{9689}, M_{9941}, and M_{11213}, were discovered by the electronic computer Illiac III at the Digital Computer Laboratory of the University of Illinois. This bring to 23 the number of known Mersenne primes which are

2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11,213.

A *multiply perfect number* is an integer n the sum of whose factors is a multiple of n. For example, the sum of the "proper" factors of 120 is twice 120, or 240; thus $1 + 2 + 3 + 4 + 5 + 6 + 8 + 10 + 12 + 15 + 20 + 24 + 30 + 40 + 60 - 240$.

Perfect Numbers

Constance Reid

The Greeks, greatly intrigued by the fact that the number 6 is the sum of all its divisors except itself (1 + 2 + 3), called it a "perfect" number. They wondered how many other such numbers there were. It was easy enough to ascertain by trial that the second perfect number was 28 (1 + 2 + 4 + 7 + 14). The great Euclid was able to prove that in all cases where a number can be factored into the form $2^{n-1}(2^n - 1)$ and $2^n - 1$ is a prime number, the number must be the sum of all its divisors except itself. Thus in the case of 6, n is 2 and $2^n - 1 = 3$, a prime number; in the case of 28, n is 3 and $2^n - 1 = 7$, again a prime number. With Euclid's formula it was no difficult matter to compute that the third and fourth perfect numbers were 496 ($n = 5$) and 8,128 ($n = 7$). But beyond that the computation became laborious, and in any event it was not proved that this rule included all the perfect numbers. Euclid left for future mathematicians a challenging question: How many perfect numbers are there?

In more than 2,000 years mathematicians were able to turn up only 12 numbers that met the strict requirements for numerical perfection. Within the past year, however, the University of California mathematician R. M. Robinson has, with the aid of a modern computer, discovered five more. The discovery did not attract the attention of the press. Perfect numbers are not useful in the construction of atomic bombs. In fact, they are not useful at all. They are merely interesting, and their story is an interesting one.

For many centuries philosophers were more concerned with the ethical or religious significance of perfect numbers than with their mathematics. The Romans attached the number 6 to Venus, because it is the product of the two sexes—the odd (masculine) number 3 and the even (feminine) number 2. The ancient Hebrews explained that God chose to create the world in six days rather than in one because 6 is the more perfect number. The eighth-century English theologian Alcuin pointed out that the second origin of the human race, from the eight human beings on Noah's Ark, was less perfect than the first, 8 being an imperfect number. In the 12th century Rabbi Josef Ankin recommended the study of perfect numbers in a program for the "healing of souls."

The mathematicians, meanwhile, had been making slow progress. The first four perfect numbers—6, 28, 496 and 8,128—had been known as early as the first century. Not until 14 centuries later was the fifth discovered. It was 33,550,336 ($n = 13$). Then in 1644 the French mathematician Marin Mersenne, a colleague of Descartes, announced six more at one clip, and thereby linked his name forever with perfect numbers. The numbers were now so large that they were necessarily described only by the prime-number $2^n - 1$, or, more briefly, by the exponent, n, in Euclid's formula. The values of n for the 11 perfect numbers, including Mersenne's six new ones, were 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 and 257. In other words, the largest prime in the series was the enormous number $2^{257} - 1$.

It was obvious to other mathematicians that Mersenne could not have tested for primality all the numbers he had announced. But neither could they. At that time the only method of testing was to try every possible divisor of each number. By this laborious method mathematicians did test Mersenne's first eight numbers and found them prime.

It was the great Swiss mathematician Leonhard Euler who tested the eighth number ($2^{31} - 1$). Euler also proved that all even perfect numbers must be of the form expressed by Euclid's theorem. No odd perfect number has ever been found, but it has never been proved that such a number cannot exist.

For more than 100 years the perfect number formed from the prime $2^{31} - 1$ remained the largest proved. Then in 1876 the French mathematician Eduard Lucas worked out a method by which a possible prime could be tested without trying all potential divisors. At the same time he announced that he had tested $2^{127} - 1$ by his method and found it prime.

According to Lucas, the number $2^n - 1$ is prime if, and only if, it divides the ($n - 1$) term of a certain series. In this series the first number is 4 and each succeeding number is the square of the preceding one minus 2; in other words 4, 14, 194, 37,634, and so on. For example, to test the prime number 7 ($2^3 - 1$), one divides 7 into 14; the $n - 1$ term in this case being the second number in the series, since n is 3. Since 7 divides evenly into 14, it is prime by Lucas' test.

Obviously even Lucas' short-cut method becomes rather unwieldy when, as in the case of $2^{127} - 1$, one must divide 170,141,183,460,469,-231,731,687,303,715,884,105,727 into the 126th term of Lucas' series. For such numbers, mathematicians use a short-cut of the short-cut: instead of squaring each term of the series, they square only the remainder after they have divided the number being tested into it.

Even with the help of Lucas' method mathematicians were not able to finish testing all of the possible Mersenne numbers until a few years ago. Their tally showed that Mersenne's list of perfect numbers was incorrect. He was right on nine numbers (those for which n is 2, 3, 5, 7, 13, 17, 19, 31 and 127), but he was wrong on two he had listed (those with the exponents 67 and 257), and he had missed three numbers in the series (with exponents 61, 89 and 107). Thus the list stood at 12, with $2^{126}(2^{127} - 1)$ the largest known perfect number.

$$
\begin{gathered}
2(2^{2} - 1) \\
2^{2}(2^{3} - 1) \\
2^{4}(2^{5} - 1) \\
2^{6}(2^{7} - 1) \\
2^{12}(2^{13} - 1) \\
2^{16}(2^{17} - 1) \\
2^{18}(2^{19} - 1) \\
2^{30}(2^{31} - 1) \\
2^{60}(2^{61} - 1) \\
2^{88}(2^{89} - 1) \\
2^{106}(2^{107} - 1) \\
2^{126}(2^{127} - 1) \\
2^{520}(2^{521} - 1) \\
2^{606}(2^{607} - 1) \\
2^{1278}(2^{1279} - 1) \\
2^{2202}(2^{2203} - 1) \\
2^{2280}(2^{2281} - 1)
\end{gathered}
$$

LIST of perfect numbers stands at 17. The last five were added by SWAC.

Then on January 30 last year Robinson fed the problem to the National Bureau of Standards' Western Automatic Computer, known briefly as SWAC. This is a high-speed machine: it can do an addition of 36 binary digits in 64 millionths of a second. Robinsons' job was to break down the Lucas method into a program of the 13 kinds of commands to which the SWAC responds. The job was complicated by the fact that, while the machine is built to handle numbers up to only 36 binary digits, the numbers he was working with ran to 2,300 such digits. It was, he found, very much like explaining to a human being how to multiply 100-digit numbers on a desk calculator built to handle 10. To tell SWAC how to test a possible prime by the Lucas method, 184 separate commands were necessary. The same program of commands, however, could be used for testing any number of the Mersenne type from $2^{3} - 1$ to $2^{2297} - 1$.

The program of commands, coded and punched on paper tape, was placed in the machine's "memory." All that was then necessary to test the primality of any Mersenne number was to insert the exponent of the new number as it was to be tested. The machine could do the rest, even to typing out the result of the test — continuous zeros if the number was a prime.

The first number to be tested was $2^{257} - 1$, the largest of the 11 numbers announced by Mersenne. Twenty years before it had been found not prime by D. H. Lehmer, who worked two hours a day for a year with a desk calculator to do the test. It happened that this evening Lehmer himself, now the director of research at the Bureau of Standards' Institute for Numerical Analysis on the U.C.L.A. campus, was in the room. He saw the machine do in 48 seconds what had taken him an arduous 700 and some hours. But the machine got exactly the same result.

SWAC then continued on a list of larger possible primes. Mersenne had said that all eternity would not suffice to test whether a given number of 15 or 20 digits was prime. But within a few hours SWAC tested 42 numbers, the smallest of which had more than 80 digits. One by one it determined that they were not prime. Finally at 10 p.m. a string of zeros came up: the machine had found a new perfect number. Its prime was $2^{521} - 1$. Just before midnight, 13 more numbers later, another prime came up: $2^{607} - 1$. In the decimal system this is a number of 183 digits.

The machine continued testing numbers when opportunity afforded during the next few months. Last June the number $2^{1279} - 1$ was found to be prime. In October, concluding the program, it established as prime the numbers $2^{2203} - 1$ and $2^{2281} - 1$. The latter is the largest prime number, of any form, now known.

The perfect numbers of which these primes are components are, of course, much larger—so large that in comparison with them conventionally "astronomical" numbers seem microscopic. Yet, by a proof as old as Euclid, mathematicians know that these numbers are the sum of all their divisors except themselves—just as surely as they know that $6 = 1 + 2 + 3$.

They still do not know, however, how many perfect numbers there are.

FOR FURTHER READING AND STUDY

There is a vast amount of literature which deals with all aspects of the theory of numbers. The references below are a few of the readily available sources for additional information on prime numbers and perfect numbers.

PRIMES and COMPOSITES; FACTORIZATION

BALL, W. W. R. *Mathematical Recreations and Essays.* Macmillan, 1942; pp. 59–75.

BARNETT, I. A. *Some Ideas About Number Theory.* National Council of Teachers of Mathematics, 1961; pp. 4–17.

BOWERS, H. AND BOWERS, J. E. *Arithmetical Excursions.* Dover Publications, 1961; pp. 106–113.

CARNAHAN, WALTER. Methods for Systematically Seeking Factors of Numbers. *School Science and Mathematics,* vol. 52, pp. 429–435 (1952).

CARNAHAN, WALTER. Prime Numbers in Sequences. *School Science and Mathematics,* vol. 54, pp. 313–315 (1954).

DAVENPORT, H. *The Higher Arithmetic.* Harper & Bros., 1960; pp. 9–39.

GRANT, HAROLD. The Prime Number Theorem. *Scripta Mathematica,* vol. 20, pp. 235–236 (1954).

JUZUK, D. AND TUCHMAN, Z. Elementary Bounds for the Number of Primes. *Scripta Mathematica,* vol. 11, pp. 179–182 (1945).

LEHMER, D. N. History of the Problem of Separating a Number into Its Prime Factors. *Scientific Monthly,* vol. 7, pp. 227–234 (1918).

LEHMER, D. N. Hunting Big Game in the Theory of Numbers. *Scripta Mathematica,* vol. 1, pp. 229–235 (1933).

MARSHALL, W. L. Some Properties of Prime Numbers. *The Pentagon,* vol. 8, pp. 5–8 (1948).

ORE, OYSTEIN. *Number Theory and Its History.* McGraw-Hill, 1948; pp. 50–85.

RADEMACHER, H. AND TOEPLITZ, O. *The Enjoyment of Mathematics.* Princeton University Press, 1957; Chapters 1, 11, and 20.

REICHMANN, W. J. *The Fascination of Numbers.* Methuen, 1957; pp. 46–63.

STEINMAN, D. B. A Second Sequel to Eratosthenes. *Scripta Mathematica,* vol. 22, pp. 79–80 (1956).

PERFECT NUMBERS; MERSENNE NUMBERS

ARCHIBALD, R. C. Mersenne's Numbers. *Scripta Mathematica,* vol. 3, pp. 112–119 (1935).

BROWN, ALAN. Multiperfect Numbers. *Scripta Mathematica,* vol. 20, pp. 103–106 (1954).

DICKSON, L. E. Perfect and Amicable Numbers. *Scientific Monthly,* vol. 10, pp. 349–354 (April, 1921).

FRAENKEL, A. A. Perfect Numbers and Amicable Numbers. *Scripta Mathematica,* vol. 9, pp. 245–255 (1943).

KRAVITZ, SIDNEY. Mersenne Numbers. *Recreational Mathematics Magazine,* vol. 8, pp. 22–24 (April, 1962).

McCARTHY, PAUL. Odd Perfect Numbers. *Scripta Mathematica,* vol. 23, pp. 43–47 (1957).

MERSENNE PRIMES, ROBINSON PRIMES, the 19th and 20th Perfect Numbers. *Recreational Mathematics Magazine*, vol. 8, pp. 25–31 (April, 1962).

RADEMACHER, H. AND TOEPLITZ, O. *The Enjoyment of Mathematics*. Princeton University Press, 1957; Chapter 19.

REID, CONSTANCE. *From Zero to Infinity*. London: Routledge & Kegan Paul, 1956; pp. 83–96.

RIESEL, H. Mersenne Numbers. *Mathematical Tables and Other Aids to Computation*, vol. 12, pp. 207–213 (1958).

TOUCHARD, JACQUES. On Prime Numbers and Perfect Numbers. *Scripta Mathematica*, vol. 19, pp. 35–39 (1953).

UHLER, HORACE. A Brief History of the Investigations on Mersenne Numbers and the Latest Immense Primes. *Scripta Mathematica*, vol. 18, pp. 122–131 (1952).

UHLER, HORACE. Full Value of the First Seventeen Perfect Numbers. *Scripta Mathematica*, vol. 20, p. 240 (1954).

—W. L. S